



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/623,262	07/18/2003	Frederick S. M. Herz	REFH-0155	3489
7590 Frederick S. M. Herz P O Box 67 Warrington, PA 18976			EXAMINER WHIPPLE, BRIAN P	
			ART UNIT 2152	PAPER NUMBER
			MAIL DATE 09/24/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/623,262

Applicant(s)

HERZ ET AL.

Examiner

Brian P. Whipple

Art Unit

2152

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 July 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-5 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-5 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- ☐ Notice of Informal Patent Application
- ☐ Other: _____

DETAILED ACTION

1. Claims 1-5 are pending in this application and presented for examination. All previous claims were cancelled by applicant's amendment received on 8/9/07.

Claim Objections

2. As to claim 5, ln. 8, the phrase "the another medical professional" lacks antecedent basis. Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claim 1 is rejected under 35 U.S.C. 102(e) as being anticipated by Sanin et al.

(Sanin), U.S. Publication No. 2004/0210770 A1.

5. As to claim 1, Sanin discloses a method for exchange of pseudonymous personal information between two or more data storage servers or within a data storage server in which the identities of persons, associated servers and/or associated

organizations with which the personal information resides in pseudonymous, comprising:

assigning a unique identification (UID) to a person having personal information for storage ([0018], ln. 1-2; [0025], ln. 5-8 and 13-14);

registering the person as a user type with associated pseudonym ([0024], ln. 1-4; [0025], ln. 5-8; [0028], ln. 1-8) and set of rules that control the person's access to stored data (Fig. 1; Abstract, ln. 1-7; [0010], ln. 12-22; [0024], ln. 1-4; [0025], ln. 5-8);

providing a service provider identifier to the person ([0025], ln. 8-13 and 19-23) a pseudonymous proxy server providing a pseudonym (Fig. 1, "IDP"; [0025], ln. 10-13; [0028], ln. 1-8; [0029], ln. 1-6) and the service provider identifier ([0025], ln. 8-13 and 19-23) with a random factor ([0028], ln. 1-8);

transmitting a message from the person to the service provider through the pseudonymous proxy server (Fig. 1; [0032], ln. 1-4 and 11-13; [0033], ln. 7-11), wherein the pseudonymous proxy server receives the message ([0032], ln. 11-13) and, based on said set of rules that control the person's access to stored data ([0010], ln. 12-22; [0032], ln. 11-13), validates a relationship between the person, the service provider and/or a private data owner ([0033], ln. 7-11); and

said pseudonymous proxy server authorizing the person to view the private data owner's actual private data ([0032], ln. 1-4 and 11-13; [0033], ln. 7-11) or pseudonyms for said private data (Abstract, ln. 1-7) based on said set of rules that control the person's access to stored data of said private data owner (Abstract, ln. 1-7; [0010], ln. 12-22; [0032], ln. 11-13; [0033], ln. 7-11).

In the citations given from Sanin (the following names, Conor and Aleksey, refer to fictional users within Sanin's teachings and not prior art inventor names), the user Conor has identity information comprising a login name and password ([0025], ln. 13-14). Therefore, inherently Conor has been assigned a unique identification, as authentication would fail and be meaningless if multiple users were assigned identical login names. It is known in the art that a login name must be unique to be valid for the purposes of authentication. Therefore, Sanin discloses assigning a unique identification to a person.

Additionally, Conor runs a calendar service ([0025], ln. 5-8). The calendar service inherently stores personal information, such as identification information in order to link itself to Conor, and scheduling information ([0033], ln. 7-11).

The user Aleksey is registered with Conor through the use of a randomly generated access code that does not disclose Aleksey's identity ([0024], ln. 1-4; [0025], ln. 5-8; [0028], ln. 1-8). Therefore, Aleksey is a person registered as a user with an associated pseudonym.

Additionally, Conor's access to Aleksey's calendar service is controlled through the use of access codes ([0024], ln. 1-4; [0025], ln. 5-8; [0028], ln. 1-8).

Furthermore, access is controlled via a combination of information sent either to Aleksey, Conor, the corresponding calendar services, or the IDP; namely, Conor and Aleksey's access codes, Conor's identity information (login name and password), Conor's service assertion, and Conor's requested display name for Aleksey ([0025], ln. 8-10; [0032], ln. 1-13; [0033], ln. 7-11).

Thus, a set of rules is employed to control access.

Aleksey's calendar service is provided to Conor. Conor stores a display name representing the calendar service of Aleksey in his calendar service ([0025], In. 8-13 and 19-23).

Therefore, a service provider identifier is provided in that the calendar service identifier is provided.

The IDP is a pseudonymous proxy server in that it masks Aleksey's identification information from Conor (Abstract, In. 1-7; Fig 1; [0028], In. 1-8). While the applicant claims the proxy server providing a pseudonym and a service provider identifier with a random factor, the applicant does not specify whether the random factor corresponds to the service provider identifier, the pseudonym, or both. Therefore, the examiner may interpret the limitation to read "a pseudonymous proxy server providing a pseudonym with a random factor and the service provider identifier", as this meets the language of providing a pseudonym and a service provider identifier with a random factor.

Before an appointment can be scheduled between Conor and Aleksey, the IDP verifies a message from Conor comprising Conor and Aleksey's access codes and the results of this verification are sent to Aleksey (Fig. 1; [0032], In. 1-4 and 11-13; [0033], In. 7-11).

Additionally, a relationship is validated between Conor, Conor and Aleksey's calendar services, and Aleksey. This is a relationship between a person (Conor), service providers (calendar services), and a private data owner (Aleksey).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sanin, in view of Arnold, U.S. Publication No. 2004/0199782 A1.

8. As to claim 1, Sanin discloses a method for exchange of pseudonymous personal information between two or more data storage servers or within a data storage server in which the identities of persons, associated servers and/or associated organizations with which the personal information resides in pseudonymous, comprising:

assigning a unique identification (UID) to a person having personal information for storage ([0018], ln. 1-2; [0025], ln. 5-8 and 13-14);

registering the person as a user type with associated pseudonym ([0024], ln. 1-4; [0025], ln. 5-8; [0028], ln. 1-8) and that control the person's access to stored data (Fig. 1; Abstract, ln. 1-7; [0024], ln. 1-4; [0025], ln. 5-8);

providing a service provider identifier to the person ([0025], ln. 8-13 and 19-23)

Art Unit: 2152

a pseudonymous proxy server providing a pseudonym (Fig. 1, "IDP"; [0025], ln. 10-13; [0028], ln. 1-8; [0029], ln. 1-6) and the service provider identifier ([0025], ln. 8-13 and 19-23) with a random factor ([0028], ln. 1-8);

transmitting a message from the person to the service provider through the pseudonymous proxy server (Fig. 1; [0032], ln. 1-4 and 11-13; [0033], ln. 7-11), wherein the pseudonymous proxy server receives the message ([0032], ln. 11-13) and, based on said control of the person's access to stored data ([0032], ln. 11-13), validates a relationship between the person, the service provider and/or a private data owner ([0033], ln. 7-11); and

said pseudonymous proxy server authorizing the person to view the private data owner's actual private data ([0032], ln. 1-4 and 11-13; [0033], ln. 7-11) or pseudonyms for said private data (Abstract, ln. 1-7) based on control of the person's access to stored data of said private data owner (Abstract, ln. 1-7; [0032], ln. 11-13; [0033], ln. 7-11).

Sanin discloses controlling a person's access to stored data (Fig. 1; Abstract, ln. 1-7), but may be interpreted as being silent on a set of rules being used to perform this step.

Similarly, Sanin discloses validating a relationship ([0032], ln. 11-13; [0033], ln. 7-11), but may be interpreted as being silent on doing so through the use of a set of rules.

Finally, Sanin discloses said pseudonymous proxy server authorizing the person to view the private data owner's actual private data ([0032], ln. 1-4 and 11-13; [0033], ln. 7-11) or pseudonyms for said private data (Abstract, ln. 1-7) based on control of the person's access to stored data of said private data owner (Abstract, ln. 1-7; [0032], ln.

Art Unit: 2152

11-13; [0033], ln. 7-11), but may be interpreted as being silent on doing so through the use of a set of rules.

However, Arnold discloses using a set of rules to control a person's access to stored data ([0037], ln. 1-14) thus validating a relationship ([0026], ln. 2-5) and allowing access to private data ([0027], ln. 1-3).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Sanin by using a set of rules as taught by Arnold in order to define multiple conditions related to private data access. For example, it may be desired to give a user no, limited, or full access to data based on conditions such as whether or not a user is of a certain authority (e.g. attending physician in Arnold's teachings; [0026], ln. 1-15; [0027], ln. 1-9) while other data objects may be allowed full access by any physician, for example.

9. As to claim 4, Sanin and Arnold disclose the invention substantially as in parent claim 1, including the person encrypting said pseudonym (Sanin: [0025], ln. 13-14; [0027], ln. 1-9; [0029], ln. 4-11; A network, LAN, or system administrator defines rules that govern the encryption of data in the network.).

10. Claims 1 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Christ et al. (Christ), DE 10327291 A1, in view of Sanin.

Art Unit: 2152

11. As to claim 1, Christ discloses a method for exchange of pseudonymous personal information between two or more data storage servers or within a data storage server in which the identities of persons, associated servers and/or associated organizations with which the personal information resides in pseudonymous (Abstract), comprising:

assigning a unique identification (UID) to a person having personal information for storage ([0002]; The patient name is a unique identification assigned to a person.); registering the person as a user type with associated pseudonym and set of rules that control the person's access to stored data ([0020]; [0024]);

providing a service provider identifier to the person ([0002]; The name of the treating physician is a service provider identifier.);

a pseudonymous proxy server providing a pseudonym and the service provider identifier (Fig. 1, item 3; [0020]);

transmitting a message from the person to the service provider through the pseudonymous proxy server (Fig 1; [0031] - [0032]; The second institution must go through the policy data base 8, which is a part of the system 3, in order to communicate with the first institution.), wherein the pseudonymous proxy server receives the message and, based on said set of rules that control the person's access to stored data, validates a relationship between the person, the service provider and/or a private data owner (Fig. 1; [0031] – [0032]); and

said pseudonymous proxy server authorizing the person to view the private data owner's actual private data or pseudonyms for said private data based on said set of

Art Unit: 2152

rules that control the person's access to stored data of said private data owner ([0031] – [0032]).

Christ discloses a pseudonymous proxy server providing a pseudonym and the service provider identifier (Fig. 1, item 3; [0020]), but is silent on doing so with a random factor. Though, it may be interpreted that the alias generated by the system is random, as otherwise this would defeat the purpose of pseudonyms to protect confidentiality.

Additionally, Sanin discloses a pseudonymous proxy server providing a pseudonym and the service provider identifier with a random factor ([0028], ln. 1-8).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Christ by using a random factor as taught by Sanin in order to strengthen the protection of confidentiality.

12. As to claim 5, Christ and Sanin disclose the invention substantially as in parent claim 5, including the pseudonymous personal information is the person's medical records (Christ: [0002]) and the data storage servers are controlled by respective medical service providers (Christ: Fig. 1; [0031] – [0032]; [0041]), where said person and said respective medical service providers are permitted access to said person's medical records based on said set of rules (Christ: [0031] – [0032]. A patient is be permitted access to his or her own medical records.), and wherein a transfer of said patient's medical records from one medical service provider to another includes the replacing of the another medical service provider's name with a pseudonym (Christ: [0020]), pseudonymizing the person's medical records in accordance with the another

Art Unit: 2152

service provider's access rights (Christ: [0020]; [0024]), and providing the access rights to the another medical professional based on authorization to the person's medical records as granted by the person (Christ: [0031] – [0032]; A patient must provide permission for the treating institution or physician to disclose medical records legally.).

13. Claims 2-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sanin as applied to claim 1 above, in view of what is well known in the art.

14. As to claim 2, Sanin discloses the invention substantially as in parent claim 1, including the pseudonymous proxy server controls unique identifications (UIDS) ([0025], ln. 13-14) and sets of rules for respective persons among multiple servers (Fig. 1; [0025], ln. 8-10; [0032], ln. 1-13; [0033], ln. 7-11; The calendar services may be interpreted as servers.).

Sanin is silent on a hub and spoke network configuration.

However, a hub and spoke network topology is extremely well known in the art. Hub and spoke networks are a desirable alternative to ring networks in that network failure is reduced through decentralizing whereas in a ring network a single point of failure could bring down a network.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Sanin by using a hub and spoke network configuration as is extremely well known in the art in order to reduce the likelihood of network failure.

15. As to claim 3, the claim is rejected for the same reasons as claim 2 above.

16. Claims 2-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sanin and Arnold as applied to claim 1 above, in view of what is well known in the art.

17. As to claim 2, Sanin and Arnold disclose the invention substantially as in parent claim 1, including the pseudonymous proxy server controls unique identifications (UIDS) (Sanin: [0025], ln. 13-14) and sets of rules for respective persons among multiple servers (Arnold: [0037], ln. 1-14; Sanin: Fig. 1; [0025], ln. 8-10; [0032], ln. 1-13; [0033], ln. 7-11; The calendar services may be interpreted as servers.).

Sanin and Arnold are silent on a hub and spoke network configuration.

However, a hub and spoke network topology is extremely well known in the art. Hub and spoke networks are a desirable alternative to ring networks in that network failure is reduced through decentralizing whereas in a ring network a single point of failure could bring down a network.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Sanin and Arnold by using a hub and spoke network configuration as is extremely well known in the art in order to reduce the likelihood of network failure.

18. As to claim 3, the claim is rejected for the same reasons as claim 2 above.

19. Claims 2-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Christ and Sanin as applied to claim 1 above, in view of what is well known in the art.

20. As to claim 2, Christ and Sanin disclose the invention substantially as in parent claim 1, including the pseudonymous proxy server controls unique identifications (UIDS) (Christ: [0020]; Christ controls unique identifications by aliasing them.) and sets of rules for respective persons among multiple servers (Fig. 1; [0020]; [0024]; [0031] – [0032]).

Christ and Sanin are silent on a hub and spoke network configuration.

However, a hub and spoke network topology is extremely well known in the art. Hub and spoke networks are a desirable alternative to ring networks in that network failure is reduced through decentralizing whereas in a ring network a single point of failure could bring down a network.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Christ and Sanin by using a hub and spoke network configuration as is extremely well known in the art in order to reduce the likelihood of network failure.

21. As to claim 3, the claim is rejected for the same reasons as claim 2 above.

22. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sanin as applied to claim 1 above, in view of what is well known in the art.

23. As to claim 4, Sanin discloses the invention substantially as in parent claim 1, but is silent on the person encryption said pseudonym.

However, encryption is extremely well known in the art. Encryption adds an extra layer of security, which is all the more important in teachings geared toward pseudonyms to protect data, such as in Sanin.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Sanin by having a person encrypt a pseudonym as is extremely well known in the art in order to add an extra layer of security to the protected data.

24. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Christ as applied to claim 1 above, in view of what is well known in the art.

25. As to claim 4, the claim is rejected for the same reasons as explained for Sanin and what is well known in the art as applied to claim 4 above.

Conclusion

26. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See the Notice of References Cited (PTO-892).

Art Unit: 2152


27. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brian P. Whipple whose telephone number is (571) 270-1244. The examiner can normally be reached on Mon-Fri (8:30 AM to 5:00 PM EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bunjob Jaroenchonwanit can be reached on (571) 272-3913. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

BPW

Brian P. Whipple
9/8/07


BUNJOB JAROENCHONWANIT
SUPERVISORY PATENT EXAMINER
9/17/07